Acronis

Acronis Cyber Cloud

Integration with N-able N-central

Integration Guide

REVISION: 4/26/2022
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Glossary</td>
<td>4</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>5</td>
</tr>
<tr>
<td>Permissions and roles</td>
<td>6</td>
</tr>
<tr>
<td>How the integration works</td>
<td>7</td>
</tr>
<tr>
<td>API configuration</td>
<td>8</td>
</tr>
<tr>
<td>Support for on-premise installations</td>
<td>8</td>
</tr>
<tr>
<td>Setup</td>
<td>9</td>
</tr>
<tr>
<td>Apply company mapping</td>
<td>10</td>
</tr>
<tr>
<td>Upload scripts and configure properties</td>
<td>12</td>
</tr>
<tr>
<td>Usage of macOS scripts</td>
<td>13</td>
</tr>
<tr>
<td>Deploy Acronis Cyber Protection agent for Windows</td>
<td>14</td>
</tr>
<tr>
<td>Uninstall the Acronis Cyber Protection agent for Windows</td>
<td>15</td>
</tr>
<tr>
<td>Install the Acronis agent to a Domain Controller</td>
<td>16</td>
</tr>
<tr>
<td>Manage protection plans (Windows)</td>
<td>17</td>
</tr>
<tr>
<td>Perform Acronis scans and tasks (Windows)</td>
<td>18</td>
</tr>
<tr>
<td>Monitor Windows devices</td>
<td>19</td>
</tr>
<tr>
<td>Disable the integration</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

This document describes how to enable and configure the integration of Acronis Cyber Cloud with N-able N-central.

Once set up, the integration enables you to:

- Deploy Acronis on Windows devices
- Map Acronis customer tenants to N-able N-central customers
- Monitor protected devices
- Apply and revoke protection plans
- Run the following types of automated tasks - backup, antivirus scan, malware scan, vulnerability assessment and patch management

All this functionality is available from within N-able N-central, without having to go to the Acronis Cyber Protect web interface.
Glossary

- **MSP** - a Managed Service Provider, who uses both N-able N-central and Acronis Cyber Protect
- **Customer** - a client of the MSP
- **Partner tenant** - the account for an MSP on Acronis Cyber Cloud
- **Customer tenant** - the account for a Customer on Acronis Cyber Cloud
Prerequisites

To use this integration, you should have:

- At least a single, fully configured N-able N-central account
- An Acronis Cyber Cloud account with:
  - at least one Customer tenant set up
  - an active user with Acronis administration permissions
  - at least one protection plan configured to be used as the default one
Permissions and roles

Only partner tenant users with Company Administrator roles are allowed to enable/disable or edit the integration.

All other users have Read-only access. This means that they can view, but not modify the integration settings.
How the integration works

In N-central, the MSPs most often use custom properties together with Automation Manager policies that pull in the appropriate customer or device-specific information, rather than creating separate Automation Manager policies per customer or per device.

In this particular integration, you should define two custom properties:

- "Acronis Registration Token" - this property's value will be automatically populated over API from the Acronis Cloud. The value will be generated once customer mapping is applied/created. This advanced feature will be supported only for Windows OS as .amp files (automation policies) work on Windows only.

- "Acronis Data Center URL" - this is the Acronis URL (without '/' at the end), which is visible in a browser when logged in the Acronis Management portal. This property's value has to be entered one time only and can then be re-used multiple times when running an integration script/Automation policy.

Once the Acronis N-central customer mapping is applied, every 10 minutes the integration will create a new registration token for each mapped customer. If a default plan is selected, the token for this plan will include 'Apply protection plan'. If no default plan is selected, then the token will be just a registration one. Once the token is created, its value will be stored in Custom Property via an API call for that customer in N-central, so that the integration scripts can automatically use this token when executed.
API configuration

1. Go to Acronis Management portal > Integrations.
2. Click on the N-able N-central tile.
3. Enter your integration credentials:
   - N-central URL
   - Username
   - Password

Support for on-premise installations

The Acronis integration for N-able N-central does support on-premise installations. In such cases, verify that the following requirements are met:

- The SSL certificate on your Web server is correctly installed, valid, trusted and doesn't produce any errors. For example, use any of the following checkers:
  - https://whatsmychaincert.com/
  - https://www.sslshopper.com/ssl-checker.html
- The default port used by the integration is TCP 443, so make sure that it is open in your firewall. The same applies if your on-premise installation is configured to use a different port.
- HTTP schema is not supported. Your installation can use HTTPS only.
Setup

In order to set up Acronis integration for N-able N-central, you have to do the following:

1. Go to Acronis Management portal > Integrations.
2. Click on the N-able N-central tile.
3. Download the Acronis_N-Central_Integration.zip file from the Download Scripts tab.
Apply company mapping

1. Go to Acronis > Customer Mapping tab.
2. Use the list to select a customer that is not currently mapped.
3. Click the Map to existing customer tenant button in the action bar to display a popup with available customer tenants and some user fields.
4. Select an unmapped customer tenant and a user account, then click Map.
   The user selected for setting default protection plan should have Acronis administration permissions.

5. Click Set default protection plan in the action bar to display a popup with available protection plans.

6. Select a default protection plan, then click Set.
**Note**

Once you have mapped an Acronis Customer tenant to N-able N-central, you have the possibility to re-map it to another customer. To achieve that use the following workflow:

- Run uninstall script (See the Uninstall chapters)
- Re-map customer in Acronis Cloud UI
- Run install script (See the Deploy chapters)
Upload scripts and configure properties

1. Go to N-able N-central > Configuration > Scheduled Tasks > Script/Software Repository.
2. Click Add and select Automation policy script type from the list.
3. Click Browse to locate the script file, downloaded from Acronis.
4. In the Name field, provide one that is similar to the script's file name (to be easily recognizable), then click OK.

Note
There is a total of 5 scripts in the zip file: Acronis Install Agent, Acronis Uninstall Agent, Acronis Manage Protection Plan, Acronis Monitoring and Acronis Scans.

5. All files with .amp extension represent N-able N-central Automation policies and are supported only for Windows OS.
   a. Log into your N-able N-central instance.
   b. Click Administration > Custom Properties.
   c. Click Add > By Customers > Text Type.
   d. Provide the following name: Acronis Registration Token.
   e. Leave empty the default text value of the property.
   f. Select the Customers and Sites that the new property will apply to.
   g. Click Save.
   h. Repeat the same procedure to create Custom Properties with:
      name: "Backup" (or similar), Default Text: "backup"
      name: "AV_scan" (or similar), Default Text: "av_scan"
      name: "Malware_scan" (or similar), Default Text: "malware_scan"
      name: "Vulnerability_assessment" (or similar), Default Text: "vulnerability_assessment"
      name: "Patch_management" (or similar), Default Text: "patch_management"
      name: "Acronis Data Center URL" but this time the property should be of URL type.
      Enter the URL of the Acronis data center as default text value, without the “/” at the end of the URL.

Note
Under the Customers tab, it is recommended to set the “Propagate to all new Customers/Sites” value using the drop-down list.
# Usage of macOS scripts

The following set of macOS scripts are used by the integration of Acronis Cyber Cloud with N-able N-central to deliver various activities:

<table>
<thead>
<tr>
<th>Script name</th>
<th>Functionality</th>
<th>Necessary arguments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronis_scans</td>
<td>Run one of the following tasks on the current device:</td>
<td>What task to run</td>
</tr>
<tr>
<td></td>
<td>• Run a backup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Run antivirus scan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Run malware scan</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Run vulnerability assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Run patch management</td>
<td></td>
</tr>
<tr>
<td>Acronis_monitoring</td>
<td>This script takes all Acronis agent alerts for the device where it runs and inserts them into the AcronisAlerts.log file, located in the same folder where the script is run</td>
<td>None</td>
</tr>
<tr>
<td>Acronis_manage_protection_plan</td>
<td>• Apply protection plan</td>
<td>• Registration token</td>
</tr>
<tr>
<td></td>
<td>• Revoke protection plan</td>
<td>• Toggle to set Yes/No</td>
</tr>
<tr>
<td>Acronis_install_agent</td>
<td>• Download installer</td>
<td>• Registration token</td>
</tr>
<tr>
<td></td>
<td>• Execute installer</td>
<td>• Data center URL</td>
</tr>
<tr>
<td></td>
<td>• Register agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Optionally, if we have a management token:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>◦ Apply protection plan</td>
<td></td>
</tr>
<tr>
<td>Acronis_uninstall_agent</td>
<td>Uninstall Acronis agent</td>
<td>None</td>
</tr>
</tbody>
</table>
Deploy Acronis Cyber Protection agent for Windows

1. In the N-able N-central interface, go to All devices.
2. Select a Windows device.
3. Click Add task > Run an Automation policy.
4. Under Repository Item, select Acronis Install Agent.
5. The value for the Acronis Cloud URL parameter can be selected from a drop-down menu or entered manually.
6. The value for the Acronis Registration Token parameter can be selected from the drop-down list. It will be populated via API call from the Acronis Cyber Protect Cloud platform, if Company mapping was performed properly as described in the previous chapter.
7. Select target devices.
8. Run the script.
Uninstall the Acronis Cyber Protection agent for Windows

1. In the N-able N-central interface, go to All devices.
2. Select a Windows device.
3. Click Add task > Run an Automation policy.
4. Under Repository Item, select Acronis Uninstall Agent.
5. Select target devices.
6. Run the script.
Install the Acronis agent to a Domain Controller

Follow the steps below in order to make an Acronis agent installation on a Domain controller from within N-able N-central. The integration applies a default protection plan on the DC and the agent runs under the selected user.

1. In the N-able N-central interface, go to All devices.
2. Select a Windows domain controller device.
3. Click Add task > Run an Automation policy.
4. Under Repository Item, select Acronis Install Agent.
5. Provide a value for the Acronis Cloud URL parameter in one of the following ways:
   - select it from a drop-down menu
   - enter it manually
6. Select a value for the Acronis Registration Token parameter from the drop-down list. It will be populated via an API call from the Acronis Cyber Protect Cloud platform, if company mapping is successful.
7. To provide a value for the Domain Controller Username and Domain Controller Password parameters, either select these from the drop-down list or enter manually.
8. Run the script.
Manage protection plans (Windows)

1. Go to **All devices** in N-able N-central.
2. Select a Windows device.
3. Click **Add task > Run an Automation policy**.
4. Under **Repository Item**, select **Acronis Manage Protection Plan** (or the name of the job defined for the script file upload in "Setup" (p. 9)).
5. The **Revoke** parameter value can be manually entered. The values accepted for this parameter are "yes" (will result in revoking of the current Protection plan) and "no" (default).
6. The **Acronis Registration Token** parameter value can be selected from the drop-down list. It will be populated via an API call from the Acronis Cyber Protect Cloud platform as long as company mapping was performed properly "Apply company mapping" (p. 10).
7. Select target devices.
8. Run the script.
Perform Acronis scans and tasks (Windows)

1. Go to All devices in N-able N-central.
2. Select a Windows device.
3. Click Add task > Run an Automation policy.
4. Under Repository Item, select Acronis Scans (or the name of the job defined for the script file upload in "Setup" (p. 9)).
5. The value for the TaskType parameter can be either selected from a drop-down menu or manually provided by entering one of the below-listed values, which represent the type of task that has to be run:
   - Backup
   - AV_scan
   - Malware_scan
   - Vulnerability_assessment
   - Patch_management
6. The value for the Acronis Registration Token parameter can remain empty. It will be populated via an API call from the Acronis Cyber Protect Cloud platform provided that company mapping was performed properly as described in "Apply company mapping" (p. 10). If not, then the value for this parameter has to be generated in the Acronis Management portal and manually filled in in N-able N-central.
   See “How the integration works” (p. 7) for instructions on how to get this token.
7. Select target devices.
8. Run the script.
Monitor Windows devices

1. Go to All devices in N-able N-central and select a Windows device.
2. Click Add task > Run an Automation policy.
3. Under Repository Item, select Acronis Monitoring (or the name of the job defined for the script file upload in "Setup" (p. 9)).
4. Select target devices.
5. Go to the Schedule tab and set a time for N-able N-central to run the task in a recurring manner.
6. Run the script.
7. Click Views > All Devices.
8. Click the name of the device to set up Windows Event Log Monitoring.
9. Navigate to the Monitoring tab and click Add.
10. Make sure that Local Agent is selected in the Monitoring Appliance drop-down list.
11. In the Services list, set the number of instances of the Windows Event Log service to 1 and click Apply.
12. Click Windows Event Log in the Service list.
13. Navigate to the Service Details tab to configure the monitoring options.
14. In Options To Monitor, select the Error, Information and Warning checkboxes for Application.
15. Configure the threshold settings in the Thresholds tab according to your personal preferences and click OK.
16. The Acronis alerts will be available on the Reports tab when filtering by Application type of events with Error, Information and Warning Event Levels. Look for Events with Acronis Agent Event Source.
Disable the integration

To completely disable the integration, the following is required:

1. In the Acronis Management portal, go to Integrations.
2. On the N-able N-central integration tile, click on the three dots (...) in the top-right and select Delete from the drop-down menu.
3. Confirm your selection.

The integration will be disabled and all mapped accounts - disconnected.

Note
Any Acronis Customer tenants, including their workloads and usages, will not be affected by this action.